ELSEVIER

Available at www.ElsevierMathematics.com POWERED BY SCIENCE DIRECT®

Finite Fields and Their Applications 10 (2004) 506–521

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

# Primitive polynomial with three coefficients prescribed ☆

Shuqin Fan* and Wenbao Han

*Department of Applied Mathematics, College of Information Engineering, Information Engineering University, Zhengzhou 450002, People's Republic of China*

Received 19 June 2003; revised 1 October 2003

Communicated by Stephen D. Cohen

**Abstract**

The authors proved in Fan and Han (Finite Field Appl., in press) that, for any given $(a_1, a_2, a_3) \in F_q^3$, there exists a primitive polynomial $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n$ over $F_q$ of degree $n$ with the first three coefficients $\sigma_1, \sigma_2, \sigma_3$ prescribed as $a_1, a_2, a_3$ when $n \geqslant 8$. But the methods in Fan and Han (in press) are not effective for the case of $n = 7$. Mills (Existence of primitive polynomials with three coefficients prescribed, J. Algebra Number Theory Appl., in press) resolves the $n = 7$ case for finite fields of characteristic at least 5. In this paper, we deal with the remaining cases and prove that there exists a primitive polynomial of degree 7 over $F_q$ with the first three coefficient prescribed where the characteristic of $F_q$ is 2 or 3.


*MSC:* 11T06; 11T71; 11L07

*Keywords:* Finite field; Galois ring; Primitive polynomial; Character sums over Galois ring

## 1. Introduction

Let $F_q$ be a finite field with $q = p^k$ elements where $p$ is a prime number and $k$ a positive integer. A monic polynomial $f(x) \in F_q[x]$ of degree $n$ is called a primitive polynomial if the least positive integer $T$ such that $f(x) | x^T - 1$ over $F_q[x]$ is $q^n - 1$. Primitive polynomials over finite fields are of great interest because of their various applications in cryptography, coding theory and digital watermarking technique, etc.

☆ This work was supported by NSF of China with Contracts 19971096 and 90104035.

* Corresponding author. Fax: +371 35 31554.

*E-mail addresses:* sq.fan@263.net (S. Fan), wb.han@netease.com (W. Han).

1071-5797/$ - see front matter 
doi:10.1016/j.ffa.2003.10.003

In some applications, we may need primitive polynomials with some special properties, and so it is very interesting to know whether for any given $q$ and $n$ there exists a primitive polynomial of degree $n$ over $F_q$ with one or several coefficients prescribed as one or several given values. For example, Hansen and Mullen [12] proposed a conjecture on the existence of primitive polynomials with one coefficient prescribed.

**Hansen–Mullen Conjecture.** *For any given element $a \in F_q$, there exists a primitive polynomial $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n$ of degree $n$ over $F_q$ with the $m$th $(0 < m < n)$ coefficient $\sigma_m = a$ except when*

$$(q, n, m, a) = (4, 3, 1, 0), (4, 3, 2, 0), (2, 4, 2, 1).$$

For $m = 1$, the Hansen–Mullen conjecture is true by the work of Jungnickel and Vanstone [13], and Cohen [2]. The case of $m = 2$ is resolved by Han in [9,11]. Recently, Fan and Han [6] proved that for $1 \leqslant m < n$, there exists a primitive polynomial over $F_q$ of degree $n$ with the $m$th coefficient prescribed except when $m = \frac{n+1}{2}$ if $n$ is odd and when $m = \frac{n}{2}, \frac{n}{2} + 1$ if $n$ is even for $q$ large enough. They even proved in [8] that the Hansen–Mullen conjecture over finite fields of characteristic two is true when $n \geqslant 7, n$ is odd.

In an excellent survey paper on primitive elements and polynomials, Cohen [3] discussed the existence of primitive polynomials with several coefficients prescribed and asked the following question:

**Cohen's Problem.** Whether there is some function $c(n)$ (such as $\frac{n}{4}$, $\sqrt{n}$, $\log n$, etc.) such that there exists a primitive polynomial over $F_q$ of degree $n$ with $\lfloor c(n) \rfloor$ coefficients prescribed.

With the help of a formula derived from Newton's identities, character sums over finite fields and a sieve technique originating from Cohen [2,3], Han [9], Cohen and Mills [4] proved that if the characteristic of $F_q$ is odd, there exists a primitive polynomial of degree $n$ over $F_q$ with the first two coefficients prescribed for $n \geqslant 7$ and $n = 5, 6$ respectively. Using the same methods, one can prove in principle that there exists a primitive polynomial of degree $n$ over $F_q$ with the first $m$ coefficients prescribed for $n > 2m$ provided that the characteristic of $F_q$ is larger than $m$ [10]. In other words, as one increases the number of prescribed coefficients, one is forced to exclude more finite fields whose characteristic is small. The authors of this paper resolved the problem by using some $p$-adic methods [5,7], as they are able to deal with all the cases which are independent of the finite field's characteristic. They obtain

**Theorem A** (Fan and Han [7]). *For any given $n$, there exists a primitive polynomial of degree $n$ over $F_q$ with the first $\lfloor \frac{n-1}{2} \rfloor$ coefficients prescribed for $q$ large enough.*

Theorem A shows that as an asymptotic result, $c(n)$ can be chosen to be $\frac{n-1}{2}$ when we deal with Cohen's problem. From Theorem A, if $n \geqslant 7$, there exists a primitive

polynomial over $F_q$ with the first three coefficients prescribed for $q$ large enough. Using estimates of character sums over Galois rings and some computing techniques, we have

**Theorem B** (Fan and Han [5]). *There exists a primitive polynomial of degree n over $F_q$ with the first three coefficients prescribed for $n \geqslant 8$.*

For general $q$, the methods used in [5] can only resolve the cases $n \geqslant 8$, whereas the case $n = 7$ cannot be settled because of the limited computational resources. Combining some careful character sums analysis over finite fields and the sieve method, Mills [16] resolves the $n = 7$ case for finite fields of characteristic at least 5. In this paper, we deal with the remaining cases, i.e., the case $n = 7$ for finite fields of characteristic 2 or 3. We prove that there exists a primitive polynomial of degree 7 over $F_q$ with the first three coefficient prescribed where the characteristic of $F_q$ is 2 or 3.

The paper is arranged as follows. In Section 2 we give some basic facts on character sums over Galois rings. In Section 3, we first give a theorem proved in [5] which translates the existence of primitive polynomials over finite fields of characteristic 2 or 3 with the first three coefficients prescribed into the existence of primitive element solutions of some system of equations over Galois rings. After a more careful analysis we get a better condition than what we get in [5] to decide whether the number of primitive element solutions of the system of trace equations is larger than zero or not. Finally, we use some computing techniques to get our main result in Section 4. Compared to the methods we used in [5], the computing methods in this paper are more effective and can make the bounds dramatically reduced.

## 2. Character sums over Galois rings

Let $e \geqslant 1, \mathbb{Z}_{p^e}$ be the residue ring of integers modulo $p^e$. A Galois ring $R_{e,k} = GR(p^e, k)$ is the unique Galois extension over $\mathbb{Z}_{p^e}$ of degree $k$ and can be written as $\mathbb{Z}_{p^e}[x]/(f(x))$, where $f(x)$ is a basic irreducible polynomial of degree $k$ over $\mathbb{Z}_{p^e}$, i.e., $f(x)$ is monic and $f(x) \bmod p$ is an irreducible polynomial over $F_p$. The ring $R_{e,k}$ is a local ring with unique maximal ideal $pR_{e,k}$ and $F_{p^k} \cong R_{e,k}/pR_{e,k}$, where $F_{p^k}$ is a finite field with $p^k$ elements. Denote the set of Teichmüller points of $R_{e,k}$ by $\Gamma_k = \{x \in R_{e,k} \mid x^{p^k} = x\}$. It can be shown that $\Gamma_k^* = \Gamma_k \backslash \{0\}$ is a multiplicative cyclic group and can be written as $\{1, \xi, \ldots, \xi^{p^k-2}\}$, where $\xi$ is a primitive element in $\Gamma_k^*$, i.e., an element with order $p^k - 1$. Every element $z \in R_{e,k}$ has a unique $p$-adic expansion

$$z = z_0 + pz_1 + \cdots + p^{e-1}z_{e-1}, \quad z_i \in \Gamma_k.$$

Let $n \geqslant 1$ be an integer and $\tau_k$ be the Frobenius map of $R_{e,nk}$ over $R_{e,k}$ given by

$$\tau_k(\beta) = \beta_0^{p^k} + p\beta_1^{p^k} + \cdots + p^{e-1}\beta_{e-1}^{p^k}$$

for $\beta = \sum_{i=0}^{e-1} p^i \beta_i \in R_{e,nk}$, where $\beta_i \in \Gamma_{nk}$. As we know, $\tau_k$ is the generator of the Galois group of $R_{e,nk}/R_{e,k}$ which is a cyclic group of order $n$. The trace mapping $Tr_{e,nk,k}(\cdot)$ from $R_{e,nk}$ to $R_{e,k}$ is defined via

$$Tr_{e,nk,k}(x) = x + \tau_k(x) + \cdots + \tau_k^{n-1}(x)$$

for $x \in R_{e,nk}$.

For any $a \in R_{e,k}$, define

$$\psi_a(c) = e^{2\pi i Tr_{e,k,1}(ac)/p^e}, \quad \forall c \in R_{e,k}.$$

It can be shown that $\{\psi_a\}_{a \in R_{e,k}}$ are all the additive characters of $R_{e,k}$. Especially, $\psi_1$ is called the canonical additive character and $\psi_0$ is called the trivial additive character of $R_{e,k}$ respectively.

**Lemma 1.** *Let $a \in R_{e,k}$, $\psi_1$ be the canonical additive character of $R_{e,k}$. We have for $1 \leqslant d \leqslant e$,*

$$\sum_{c \in R_{d,k}} \psi_1(p^{e-d} ca) = \begin{cases} q^d & \text{if } a = 0 \bmod p^d, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\Gamma_{nk}$ be the set of Teichmüller points of $R_{e,nk}$. As we know, $\Gamma_{nk}^* = \Gamma_{nk} \backslash \{0\}$ is a multiplicative cyclic group with $q^n - 1$ elements. Let $g$ be a fixed primitive element (i.e., generator) of $\Gamma_{nk}^*$, the canonical multiplicative character $\chi_1$ can be defined by $\chi_1(g^l) = e^{2\pi i l/q^n - 1}$ for $0 \leqslant l \leqslant q^n - 2$. For $0 \leqslant j \leqslant q^n - 2$, define $\chi_j(g^l) = \chi_1(g^{lj})$. The $\chi_j$'s are all the multiplicative characters of $\Gamma_{nk}^*$ and form a cyclic group with $q^n - 1$ elements. It is known that the order of each character $\chi_j$ is a divisor of $q^n - 1$.

Let $h(x)$ be a polynomial over $R_{e,nk}$ with $h(0) = 0$ and $h(x)$ not identically 0, and let $h(x) = h_0(x) + h_1(x)p + \cdots + h_{e-1}(x)p^{e-1}$ be the $p$-adic expansion of $h(x)$, where $h_i(x)$ is a polynomial of degree $d_i$ with coefficients in $\Gamma_{nk}$ for $i = 0, 1, \ldots, e-1$. Define the weighted $e$-degree of $h(x)$ by

$$D_{e,h} = \max(d_0 p^{e-1}, d_1 p^{e-2}, \ldots, d_{e-1}).$$

**Definition 1.** Let $h(x), h_i(x)$ be defined as above, and let $h_i(x) = \sum_{j=0}^{d_i} h_{i,j} x^j$, $h_{i,j} \in \Gamma_{nk}$. $h(x)$ is called *nondegenerate* if

$$h_{i,j} = 0, \quad \text{if } j \equiv 0 \bmod p, \ 0 \leqslant j \leqslant d_i, \quad 0 \leqslant i \leqslant e-1.$$

Next we will give two estimates of character sums over Galois rings which are analogous to Weil estimates on character sums over finite fields.

**Theorem 2** (Kumar [14], Li [15]). *Let $f(x)$ be a nondegenerate polynomial over $R_{e,nk}$ with weighted e-degree $D_{e,f}$, $\psi_{e,nk}$ a nontrivial additive character of $R_{e,nk}$ and $\chi_{nk}$ a*

*nontrivial multiplicative character of* $\Gamma_{nk}^*$. *Then*

$$\left|\sum_{\xi\in\Gamma_{nk}}\psi_{e,nk}(f(\xi))\right|\leqslant(D_{e,f}-1)q^{\frac{n}{2}}$$

*and*

$$\left|\sum_{\xi\in\Gamma_{nk}^*}\psi_{e,nk}(f(\xi))\chi_{nk}(\xi)\right|\leqslant D_{e,f}q^{\frac{n}{2}}.$$

## 3. Estimates and sieve method

Next we will give a theorem which translates the existence of primitive polynomials of degree $n$ over finite fields of characteristic 2 or 3 with the first three coefficients prescribed into the existence of primitive element solutions in $\Gamma_{nk}^*$ of some system of trace equations from $R_{2,nk}$ to $R_{2,k}$.

**Theorem 3** (Fan and Han [5]). *Let* $p=2,3$ *and*

$$m=\begin{cases}2 & \text{if } p=3,\\ 3 & \text{if } p=2.\end{cases}$$

*If the system of equations*

$$\begin{cases}Tr_{2,nk,k}(x)=a_1+pb_1,\\ Tr_{2,nk,k}(x^m)\equiv a_m \bmod p\end{cases}\tag{1}$$

*has a primitive element solution in* $\Gamma_{nk}^*$ *for any given* $a_1,b_1,a_m\in\Gamma_k$, *there exists a primitive polynomial* $f(x)=x^n-\sigma_1x^{n-1}+\cdots+(-1)^n\sigma_n$ *over* $F_q$ *of degree n with the first three coefficients* $\sigma_1,\sigma_2,\sigma_3$ *prescribed. In particular*, $\sigma_1=\sigma_2=\sigma_3=0$ *if and only if* $a_1=b_1=a_m=0$.

Now we estimate the number of primitive element solutions of (1) in $\Gamma_{nk}^*$, which we denote by $N_{q,n}(a_1,b_1,a_m)$. To get a good bound of $N_{q,n}(a_1,b_1,a_m)$, we first provide a generalization of Cohen's sieve.

Let $r\mid q^n-1$, $\xi\in\Gamma_{nk}^*$. We say $\xi$ is not any kind of $r$th power in $\Gamma_{nk}^*$ if $\xi=\rho^d,\rho\in\Gamma_{nk}^*,d\mid r$ only if $d=1$. Define

$$\mathscr{S}_r(a_1,b_1,a_m)=\{\xi\in\Gamma_{nk}^*\mid \xi \text{ is a solution of (1) and } \xi \text{ is not any kind of } r\text{th power in } \Gamma_{nk}^*\}.$$

It is obvious that $|\mathscr{S}_{q^n-1}(a_1,b_1,a_m)|=N_{q,n}(a_1,b_1,a_m)$.

**Definition 2.** Let $r \mid q^n - 1$, $r_0, r_1, r_2, \ldots, r_l$ be the divisors of $r$, satisfying: (i) $lcm(r_1, r_2, \ldots, r_l) = r$, (ii) $gcd(r_i, r_j) = r_0$, for $1 \leqslant i < j \leqslant l$. We call $r_1, r_2, \ldots, r_l$ the complementary divisors of $r$ with common divisor $r_0$.

With the above notions, we have

**Lemma 4** (Chou and Cohen [1], Fan and Han [5]). *Let $r \mid q^n - 1$, $r_1, \ldots, r_l$ be the complementary divisors of $r$ with common divisor $r_0$. Then*

$$|\mathscr{S}_r(a_1, b_1, a_m)| = |\mathscr{S}_{r_1}(a_1, b_1, a_m)| + \cdots + |\mathscr{S}_{r_l}(a_1, b_1, a_m)| - (l-1)|\mathscr{S}_{r_0}(a_1, b_1, a_m)|. \tag{2}$$

Next we give a lemma which decides whether an element $\xi$ is any kind of $r$th power in $\Gamma_{nk}^*$ or not.

**Lemma 5** (Fan and Han [5]). *Let $r \mid q^n - 1$, $\xi \in \Gamma_{nk}^*$. Then*

$$\sum_{d \mid r} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) = \begin{cases} \frac{r}{\varphi(r)} & \text{if } \xi \text{ is not any kind of } r\text{th power}, \\ 0 & \text{otherwise}, \end{cases}$$

*where $\mu(d)$ is the Möbius function and $\varphi(d)$ is the Euler function, $\chi^{(d)}$ runs through all of the $\varphi(d)$ multiplicative characters of $\Gamma_{nk}^*$ with order $d$.*

Let $\psi_{2,k}, \psi_{2,nk}$ be the canonical additive character over $R_{2,k}, R_{2,nk}$, respectively, where $\psi_{2,nk} = \psi_{2,k} \circ Tr_{2,nk,k}$. Let $\chi^{(d)}$ run through all of the multiplicative characters of $\Gamma_{nk}^*$ with order $d$. From Lemmas 1 and 5, we have

$$\begin{aligned} q^3 &|\mathscr{S}_{r_i}(a_1, b_1, a_m)| \\ &= \theta(r_i) \sum_{\xi \in \Gamma_{nk}^*} \sum_{c = c_1 + pc_p \in R_{2,k}} \psi_{2,k}(c(Tr_{2,nk,k}(\xi) - (a_1 + pb_1))) \\ &\quad \times \sum_{c_m \in \Gamma_k} \psi_{2,k}(pc_m(Tr_{2,nk,k}(\xi^m) - a_m)) \sum_{d \mid r_i} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) \\ &= \theta(r_i) \sum_{d \mid r_i} \Theta_d(a_1, b_1, a_m), \end{aligned} \tag{3}$$

where

$$\theta(r_i) = \frac{\varphi(r_i)}{r_i},$$

$$\Theta_d(a_1, b_1, a_m) = \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{c_1, c_p, c_m \in \Gamma_k} \psi_{2,k}(-c_1 a_1 - pc_p a_1 - pc_1 b_1 - pc_m a_m) \cdot \Lambda_{c_1, c_p, c_m, d}$$

and

$$\Lambda_{c_1,c_p,c_m,d} = \sum_{\xi \in \Gamma_{nk}^*} \psi_{2,nk}(c_1\xi + pc_p\xi + pc_m\xi^m)\chi^{(d)}(\xi).$$

**Theorem 6.** *Let $\Theta_d(a_1, b_1, a_m)$ be defined as above. Then the following holds*:

1. *Suppose* $(a_1, b_1, a_m) = (0, 0, 0)$. *In this case, let* $Q = \frac{q^n-1}{q-1}$.
   (a) *If* $d = 1$,

$$\Theta_1(0, 0, 0) \geqslant q^n - 1 - 3(q^3 - 1)q^{\frac{n}{2}}. \tag{4}$$

   (b) *If* $d \nmid Q$,

$$\Theta_d(0, 0, 0) = 0. \tag{5}$$

   (c) *If* $d|Q, d \neq 1$,

$$|\Theta_d(0, 0, 0)| \leqslant 3(q^3 - 1)q^{\frac{n}{2}}. \tag{6}$$

2. *Suppose* $(a_1, b_1, a_m) \neq (0, 0, 0)$.
   (a) *If* $d = 1$,

$$\Theta_1(a_1, b_1, a_m) \geqslant q^n - 1 - (9q^{\frac{n+5}{2}} + 3q^{\frac{n+4}{2}}). \tag{7}$$

   (b) *If* $d > 1$,

$$|\Theta_d(a_1, b_1, a_m)| \leqslant 9q^{\frac{n+5}{2}} + 3q^{\frac{n+4}{2}}. \tag{8}$$

**Proof.** Let $h(x) = c_1x + pc_px + pc_mx^m$. If $(c_1, c_p, c_m) = (0, 0, 0)$,

$$\psi_{2,k}(-c_1a_1 - pc_pa_1 - pc_1b_1 - pc_ma_m) = 1.$$

It is easy to verify that for $d = 1$,

$$\frac{\mu(1)}{\varphi(1)} \sum_{\chi^{(1)}} \Lambda_{0,0,0,1} = q^n - 1 \tag{9}$$

and for $d > 1$,

$$\frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \Lambda_{0,0,0,d} = \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{\xi \in \Gamma_{nk}^*} \chi^{(d)}(\xi) = 0. \tag{10}$$

On the other hand, if $(c_1, c_p, c_m) \neq (0,0,0)$, then $h(x) \neq 0, h(x)$ is a nondegenerate polynomial over $R_{2,k}$ with the weighted $e$-degree $D_{2,h} \leqslant 3$. From Theorem 2,

$$|\Lambda_{c_1,c_p,c_m,d}| \leqslant 3q^{\frac{n}{2}}.$$

Our proof is divided into the following cases:

1. $(a_1, b_1, a_m) = (0,0,0)$. In this case,

$$\Theta_d(0,0,0) = \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{c_1,c_p,c_m \in \Gamma_k} \Lambda_{c_1,c_p,c_m,d}.$$

(1.a) If $c_1 \neq 0$,

$$\sum_{\substack{c_1 \in \Gamma_k^* \\ c_p,c_m \in \Gamma_k}} \Lambda_{c_1,c_p,c_m,d} = \sum_{c_1 \in \Gamma_k^*} \chi^{(d)}(c_1^{-1}) \sum_{c_p',c_m' \in \Gamma_k} \Lambda_{1,c_p',c_m',d},$$

where $c_p' = c_p c_1^{-1}$, $c_m' = c_m c_1^{-m}$. On the other hand, the multiplicative character $\chi^{(d)}$ of $\Gamma_{nk}^*$, when restricted to $\Gamma_k^*$, is a trivial multiplicative character of $\Gamma_k^*$ iff $d|Q$. So if $d \nmid Q$,

$$\sum_{c_1 \in \Gamma_k^*} \chi^{(d)}(c_1^{-1}) = 0.$$

Since the number of multiplicative characters of $\Gamma_{nk}^*$ with order $d$ is $\varphi(d)$, we have

$$\left| \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{\substack{c_1 \in \Gamma_k^* \\ c_p,c_m \in \Gamma_k}} \Lambda_{c_1,c_p,c_m,d} \right| \leqslant \begin{cases} 0 & \text{if } d \nmid Q, \\ 3(q-1)q^2 q^{\frac{n}{2}} & \text{if } d|Q. \end{cases} \tag{11}$$

(1.b) If $c_1 = 0, c_p \neq 0$, we can similarly get

$$\left| \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{\substack{c_p \in \Gamma_k^* \\ c_m \in \Gamma_k}} \Lambda_{0,c_p,c_m,d} \right| \leqslant \begin{cases} 0 & \text{if } d \nmid Q, \\ 3(q-1)q \cdot q^{\frac{n}{2}} & \text{if } d|Q. \end{cases} \tag{12}$$

(1.c) If $c_1 = c_p = 0, c_m \neq 0$, we divide it into two subcases:

(1.c.1) $p = 2, q \equiv 1 \bmod 3$ or $p = 3$.

(i) If $p = 2, q \equiv 1 \bmod 3$ , we have $3|q-1, m = 3$. In this case, let $\alpha$ be a cubic nonresidue in $\Gamma_k^*$, $C$ be the set of cubic residues in $\Gamma_k^*$.

(ii) If $p=3$, we have $2|q-1, m=2$. In this case, let $\alpha$ be a quadratic nonresidue in $\Gamma_k^*$, $C$ be the set of quadratic residues in $\Gamma_k^*$.

In both (i) and (ii), $\Gamma_k^* = C \cup C\alpha \cup \cdots \cup C\alpha^{m-1}$. Thus

$$\begin{aligned}\sum_{c_m\in\Gamma_k^*} \Lambda_{0,0,c_m,d} &= \sum_{i=0}^{m-1} \sum_{c_m\in C} \sum_{\xi\in\Gamma_{nk}^*} \psi_{2,nk}(c_m\alpha^i\xi^m)\chi^{(d)}(\xi)\\ &= \frac{1}{m}\sum_{i=0}^{m-1} \sum_{c'_m\in\Gamma_k^*} \sum_{\xi\in\Gamma_{nk}^*} \psi_{2,nk}(\alpha^i(c'_m\xi)^m)\chi^{(d)}(\xi)\\ &= \frac{1}{m}\sum_{i=0}^{m-1} \sum_{c'_m\in\Gamma_k^*} \chi^{(d)}(c_m'^{-1}) \sum_{\xi\in\Gamma_{nk}^*} \psi_{2,nk}(\alpha^i\xi^m)\chi^{(d)}(\xi)\\ &= \frac{1}{m}\sum_{c'_m\in\Gamma_k^*} \chi^{(d)}(c_m'^{-1}) \sum_{i=0}^{m-1} \Lambda_{0,0,\alpha^i,d}, \end{aligned} \tag{13}$$

where $c_m'^m = c_m$.

(1.c.2) $p=2, q\equiv 2 \bmod 3$. In this case we have $m=3, gcd(m,q-1)=1$. So for any given $c_m\in\Gamma_k^*$, there exists a unique element $c'_m\in\Gamma_k^*$ such that $c_m = c_m'^m$. It is easy to verify

$$\sum_{c_m\in\Gamma_k^*} \Lambda_{0,0,c_m,d} = \sum_{c'_m\in\Gamma_k^*} \chi^{(d)}(c_m'^{-1})\Lambda_{0,0,1,d}. \tag{14}$$

By (13), (14), we have

$$\left|\frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{c_m\in\Gamma_k^*} \Lambda_{0,0,c_m,d}\right| \leqslant \begin{cases} 0 & \text{if } d\nmid Q,\\ 3(q-1)q^{\frac{n}{2}} & \text{if } d|Q. \end{cases} \tag{15}$$

From (9)–(12) and(15) we get (4)–(6). This finishes the proof of the first part.

2. $(a_1,b_1,a_m)\neq(0,0,0)$, where $(a_1,b_1)\neq(0,0)$.

(2.a) If $c_1\neq 0$,

$$\begin{aligned}&\sum_{\substack{c_1\in\Gamma_k^*\\ c_p,c_m\in\Gamma_k}} \psi_{2,k}(-c_1a_1 - pc_pa_1 - pc_1b_1 - pc_ma_m)\Lambda_{c_1,c_p,c_m,d}\\ &= \sum_{c_1\in\Gamma_k^*} \psi_{2,k}(-c_1(a_1+pb_1)) \sum_{c_p,c_m\in\Gamma_k} \psi_{2,k}(-pc_pa_1 - pc_ma_m)\Lambda_{c_1,c_p,c_m,d}\\ &= \sum_{\substack{c_1\in\Gamma_k^*\\ c'_p,c'_m\in\Gamma_k}} \psi_{2,k}(-c_1a_1 - pc_1(b_1+c'_pa_1) - pc_1^mc'_ma_m)\chi^{(d)}(c_1^{-1})\Lambda_{1,c'_p,c'_m,d}, \end{aligned}$$

where $c'_p = c_p c_1^{-1}, c'_m = c_m c_1^{-m}$. Let $l(x) = -a_1 x - p(b_1 + c'_p a_1)x - pc'_m a_m x^m$. It is easy to verify that $l(x) \neq 0$ if $(a_1, b_1) \neq (0,0)$. From Theorem 2, we have

$$\left| \sum_{c_1 \in \Gamma_k^*} \psi_{2,k}(-c_1 a_1 - pc_1(b_1 + c'_p a_1) - pc_1^m c'_m a_m)\chi^{(d)}(c_1^{-1}) \right|$$
$$= \left| \sum_{c_1 \in \Gamma_k^*} \psi_{2,k}(l(c_1))\chi^{(-d)}(c_1) \right| \leqslant 3q^{\frac{1}{2}}.$$

Thus

$$\left| \sum_{\substack{c_1 \in \Gamma_k^* \\ c_p, c_m \in \Gamma_k}} \psi_{2,k}(-c_1 a_1 - pc_p a_1 - pc_1 b_1 - pc_m a_m)\Lambda_{c_1,c_p,c_m,d} \right| \leqslant 9q^{\frac{n+5}{2}}. \tag{16}$$

(2.b) If $c_1 = 0, (c_p, c_m) \neq (0,0)$, from Theorem 2,

$$\left| \sum_{\substack{c_p, c_m \in \Gamma_k \\ (c_p, c_m) \neq (0,0)}} \psi_{2,k}(-c_1 a_1 - pc_p a_1 - pc_1 b_1 - pc_m a_m)\Lambda_{0,c_p,c_m,d} \right| \leqslant 3(q^2 - 1)q^{\frac{n}{2}} \leqslant 3q^{\frac{n+4}{2}}. \tag{17}$$

3. $(a_1, b_1, a_m) \neq (0,0,0)$, where $(a_1, b_1) = (0,0)$, $a_m \neq 0$.

(3.a) If $c_m \neq 0$, we divide it into two subcases as we deal with Case (1.c).

(3.a.1) $p = 2, q \equiv 1 \bmod 3$ or $p = 3$. Let $\alpha, C$ be defined as in Case (1.c.1). With the same ideas we used in Case (1.c.1), we get

$$\sum_{\substack{c_m \in \Gamma_k^* \\ c_1, c_p \in \Gamma_k}} \psi_{2,k}(-c_1 a_1 - pc_p a_1 - pc_1 b_1 - pc_m a_m)\Lambda_{c_1,c_p,c_m,d}$$
$$= \sum_{c_m \in \Gamma_k^*} \psi_{2,k}(-pc_m a_m) \sum_{c_1, c_p \in \Gamma_k} \Lambda_{c_1,c_p,c_m,d}$$
$$= \sum_{i=0}^{m-1} \sum_{c_m \in C} \psi_{2,k}(-pc_m \alpha^i a_m) \sum_{c_1, c_p \in \Gamma_k} \Lambda_{c_1,c_p,c_m\alpha^i,d}$$
$$= \frac{1}{m} \sum_{i=0}^{m-1} \sum_{c'_m \in \Gamma_k^*} \psi_{2,k}(-pc'^m_m \alpha^i a_m)\chi^{(d)}(c'^{-1}_m) \sum_{c'_1, c'_p \in \Gamma_k} \Lambda_{c'_1,c'_p,\alpha^i,d},$$

where $c'^m_m = c_m, c'_1 = c_1 c'^{-1}_m, c'_p = c_p c'^{-1}_m$.

(3.a.2) $p=2, q\equiv 2 \bmod 3$. In this case, for any given $c_m\in\Gamma_k^*$, there exists a unique element $c'_m\in\Gamma_k^*$ such that $c_m=c_m'^m$. Let $c'_1=c_1c_m'^{-1}$, $c'_p=c_pc_m'^{-1}$. It can be verified that

$$\sum_{\substack{c_m\in\Gamma_k^*\\ c_1,c_p\in\Gamma_k}}\psi_{2,k}(-c_1a_1-pc_pa_1-pc_1b_1-pc_ma_m)\Lambda_{c_1,c_p,c_m,d}$$
$$=\sum_{c'_m\in\Gamma_k^*}\psi_{2,k}(-pc_m'^ma_m)\chi^{(d)}(c_m'^{-1})\sum_{c'_1,c'_p\in\Gamma_k}\Lambda_{c'_1,c'_p,1,d}.$$

For $i=0,1,\ldots,m-1$, let $l_i(x)=-p\alpha^ia_mx^m$. Since $a_m\neq 0$, $l_i(x)$ is a nondegenerate polynomial over $R_{2,k}$ with the weighted $e$-degree $D_{e,l_i}\leqslant 3$. From Theorem 2,

$$\left|\sum_{c'_m\in\Gamma_k^*}\psi_{2,k}(-pc_m'^m\alpha^ia_m)\chi^{(d)}(c_m'^{-1})\right|\leqslant 3q^{\frac{1}{2}}.$$

Thus we have

$$\left|\sum_{\substack{c_m\in\Gamma_k^*\\ c_1,c_p\in\Gamma_k}}\psi_{2,k}(-c_1a_1-pc_pa_1-pc_1b_1-pc_ma_m)\Lambda_{c_1,c_p,c_m,d}\right|\leqslant 9q^{\frac{n+5}{2}}. \tag{18}$$

(3.b) If $c_m=0,(c_1,c_p)\neq(0,0)$, from Theorem 2,

$$\left|\sum_{\substack{c_1,c_p\in\Gamma_k\\ (c_1,c_p)\neq(0,0)}}\psi_{2,k}(-c_1a_1-pc_pa_1-pc_1b_1-pc_ma_m)\Lambda_{c_1,c_p,0,d}\right|\leqslant 3(q^2-1)q^{\frac{n}{2}}\leqslant 3q^{\frac{n+4}{2}}. \tag{19}$$

By (9), (10), (16), (17),(18), (19) we can get (7), (8). So we have finished the proof of the second part. □

**Proposition 7.** *Let $N_{q,n}(a_1,b_1,a_m)$ be the number of primitive element solutions of* (1) *in $\Gamma_{nk}^*$. Let*

$$r=\begin{cases}\dfrac{q^n-1}{q-1} & \text{if } (a_1,b_1,a_m)=(0,0,0),\\ q^n-1 & \text{if } (a_1,b_1,a_m)\neq(0,0,0).\end{cases}$$

*and $r_1,r_2,\ldots,r_l$ be the complementary divisors of $r$ with common divisor $r_0$. We have*

1. *$N_{q,n}(0,0,0)>0$ if we can choose suitable $r_0,r_1,r_2,\ldots,r_l$ such that inequalities* (20), (21) *hold.*

2. *for* $(a_1, b_1, a_m) \neq (0,0,0)$, $N_{q,n}(a_1, b_1, a_m) > 0$ *if we can choose suitable* $r_0, r_1, r_2, \ldots, r_l$ *such that inequalities* (20), (22) *hold.*

**Proof.** From Theorem 6 and Eq. (3),

$$\begin{aligned} q^3 N_{q,n}(a_1, b_1, a_m) &= \theta(q^n - 1) \sum_{d \mid q^n - 1} \Theta_d(a_1, b_1, a_m) \\ &= \theta(q^n - 1) \sum_{d \mid r} \Theta_d(a_1, b_1, a_m) \\ &= \frac{\theta(q^n - 1)}{\theta(r)} q^3 |\mathscr{S}_r(a_1, b_1, a_m)|. \end{aligned}$$

So $N_{q,n}(a_1, b_1, a_m) > 0$ if and only if $|\mathscr{S}_r(a_1, b_1, a_m)| > 0$. On the other hand, by Lemma 4,

$$\begin{aligned} & q^3 |\mathscr{S}_r(a_1, b_1, a_m)| \\ &= q^3 \sum_{i=1}^{l} |\mathscr{S}_{r_i}(a_1, b_1, a_m)| - q^3 (l-1) |\mathscr{S}_{r_0}(a_1, b_1, a_m)| \\ &= \sum_{i=1}^{l} \theta(r_i) \sum_{d \mid r_i} \Theta_d(a_1, b_1, a_m) - (l-1)\theta(r_0) \sum_{d \mid r_0} \Theta_d(a_1, b_1, a_m) \\ &= \left( \sum_{i=1}^{l} \theta(r_i) - (l-1)\theta(r_0) \right) \Theta_1(a_1, b_1, a_m) + \left( \sum_{i=1}^{l} \theta(r_i) - (l-1)\theta(r_0) \right) \\ &\quad \times \sum_{d \mid r_0, d \neq 1} \Theta_d(a_1, b_1, a_m) + \sum_{i=1}^{l} \theta(r_i) \sum_{d \mid r_i, d \nmid r_0} \Theta_d(a_1, b_1, a_m). \end{aligned}$$

Suppose that we can choose suitable $r_0, r_1, \ldots, r_l$ such that

$$\sum_{i=1}^{l} \theta(r_i) - (l-1)\theta(r_0) > 0. \tag{20}$$

From Theorem 6, it is easy to verify that for $(a_1, b_1, a_m) = (0,0,0)$, we have $N_{q,n}(0,0,0) > 0$ if

$$q^{\frac{n}{2}-3} > 3 \cdot \left( \frac{\sum_{i=1}^{l} \theta(r_i)(2^{\omega(r_i)} - 2^{\omega(r_0)})}{\sum_{i=1}^{l} \theta(r_i) - (l-1)\theta(r_0)} + 2^{\omega(r_0)} \right) \tag{21}$$

and for $(a_1, b_1, a_m) \neq (0,0,0)$, we have $N_{q,n}(a_1, b_1, a_m) > 0$ if

$$q^n - 1 > \left( \frac{\sum_{i=1}^{l} \theta(r_i)(2^{\omega(r_i)} - 2^{\omega(r_0)})}{\sum_{i=1}^{l} \theta(r_i) - (l-1)\theta(r_0)} + 2^{\omega(r_0)} \right) (9q^{\frac{n+5}{2}} + 3q^{\frac{n+4}{2}}). \tag{22}$$

In the above $\omega(r_i)$ denotes the number of distinct prime divisors of $r_i$ for $i = 0, 1, \ldots, l$. This finishes the proof. □

## 4. Computation

In this section, we assume $n = 7$. We will discuss when inequalities (20), (21) hold for $(a_1, b_1, a_m) = (0, 0, 0)$ and when inequalities (20), (22) hold for $(a_1, b_1, a_m) \neq (0, 0, 0)$ respectively. Let $r$ be defined as in Proposition 7 and let

$$r = p_1^{\gamma_1} \ldots p_s^{\gamma_s},$$

where $p_1, \ldots, p_s$ are the distinct prime divisors of $r$, $p_1 < \cdots < p_s$. For $0 \leqslant t_0 \leqslant s$, let

$$r_0 = p_1^{\gamma_1} \cdots p_{t_0}^{\gamma_{t_0}}$$

and

$$r_i = r_0 p_{t_0+i}^{\gamma_{t_0+i}},$$

where $i = 1, 2, \ldots, l = s - t_0$. It is easy to see that $r_1, r_2, \ldots, r_l$ are the complementary divisors of $r$ with common divisor $r_0$. Correspondingly, suppose that we can choose suitable $t_0$ such that

$$\sum_{i=t_0+1}^{s} \frac{p_i - 1}{p_i} - (l - 1) = 1 - \sum_{i=t_0+1}^{s} \frac{1}{p_i} > 0. \tag{23}$$

By Proposition 7, $N_{q,7}(0, 0, 0) > 0$ if we have

$$q^{\frac{1}{2}} > 3 \cdot 2^{t_0} \cdot \left( \frac{l - 1}{1 - \sum_{i=t_0+1}^{s} \frac{1}{p_i}} + 2 \right); \tag{24}$$

and when $(a_1, b_1, a_m) \neq (0, 0, 0)$, $N_{q,7}(a_1, b_1, a_m) > 0$ for $q > 9$ if

$$q > 10 \cdot 2^{t_0} \cdot \left( \frac{l - 1}{1 - \sum_{i=t_0+1}^{s} \frac{1}{p_i}} + 2 \right). \tag{25}$$

We consider the all zero case first.

**Proposition 8.** *Let $p = 2, 3$, $q$ a power of $p$. If $q \geqslant 1760$, we have $N_{q,7}(0, 0, 0) > 0$.*

**Proof.** For $(a_1, b_1, a_m) = (0, 0, 0)$ and $n = 7$, we have $r = \frac{q^7 - 1}{q - 1}$. In this case, the only possible prime divisors of $r$ are 7 or the form $14h + 1$, where $h \in \mathbb{Z}_{>0}$. We can verify

that if $\omega(r)\geqslant 266$,

$$q^6 = \frac{1}{2}\cdot(2q^6) > \frac{1}{2}\cdot r \geqslant \frac{1}{2}\times \underbrace{7\times 29\times\cdots\times 13469}_{266 \text{ primes}} \times 2^{12(\omega(r)-266)}$$
$$\geqslant 3^{12}\cdot 2^{12\omega(r)}.$$

that is, inequalities (23), (24) hold for $r_0 = r$. For $\omega(r)\leqslant 265$, let $r_0 = 1$, i.e., $t_0 = 0$, we have

$$1 - \frac{6}{7} - \frac{28}{29} - \cdots - \frac{13440}{13441} = 0.668436 > 0.$$

So if we have

$$q^{\frac{1}{2}} > 3\cdot\left(\frac{264}{0.668436} + 2\right) = 1190.86,$$

inequalities (23), (24) hold for $r_0 = 1$. It is easy to verify that $q^{\frac{1}{2}}\leqslant 1190.86$ implies $\omega(r)\leqslant 16$. For $\omega(r)\leqslant 16$, we repeat the above process as we deal with $\omega(r)\leqslant 265$ and so on. Finally we get that if $q^{\frac{1}{2}} > 41.9502$, i.e., $q\geqslant 1760$, $N_{q,7}(0,0,0) > 0$. The precise computation is listed in Table 1. □

Similarly we can get

**Proposition 9.** *Let $p = 2, 3, q$ a power of $p$. If $q\geqslant 4100$, $N_{q,7}(a_1, b_1, a_m) > 0$ for $(a_1, b_1, a_m)\neq(0,0,0)$.*

**Proof.** The proof process is similar to the proof of Proposition 8, with the only exception that the prime divisors of $q^7 - 1$ do not have any specified form. The precise computation is listed in Table 2 and the readers can verify it easily. □

From Proposition 8 we only need to discuss if $N_{q,7}(0,0,0) > 0$ for $q = 2^k, 1\leqslant k\leqslant 10$ and $q = 3^k, 1\leqslant k\leqslant 6$. Factoring $\frac{q^7-1}{q-1}$ for the above $q$'s, we find that for $q = 2^7, 2^9, 2^{10}$ and $q = 3^5, 3^6$, we can choose suitable $r_0$ such that (23), (24) hold. On the other hand, from Proposition 9, for $(a_1, b_1, a_m)\neq(0,0,0)$, we only need to consider $q = 2^k, 1\leqslant k\leqslant 12$ and $q = 3^k, 1\leqslant k\leqslant 7$. Similarly we factor $q^7 - 1$ for the above $q$'s and find that for $q = 2^7, 2^9, 2^{10}$ and $q = 3^5, 3^6$, we can choose suitable $r_0$ such that (23), (25) hold.

Combining the above results, we infer that for any given 3-tuple $(\sigma_1, \sigma_2, \sigma_3)\in F_q^3$, there exists a primitive polynomial of degree 7 over $F_q$ with the first three coefficients prescribed as $\sigma_1, \sigma_2, \sigma_3$ except that $q = 2, 4, 8, 16, 32, 64, 3, 9, 27, 81$ for all $(\sigma_1, \sigma_2, \sigma_3)\in F_q^3$ and $q = 2^8$ for $(\sigma_1, \sigma_2, \sigma_3) = (0,0,0)$.

Table 1
The sieve data for $(a_1, b_1, a_m) = (0, 0, 0)$

| $\omega(r)$ | $t_0$ | $q^{\frac{1}{2}}$ |
|---|---|---|
| 265 | 0 | 1190.86 |
| 16 | 0 | 67.0888 |
| 11 | 0 | 46.1032 |
| 10 | 0 | 41.9502 |

Table 2
The sieve data for $(a_1, b_1, a_m) \neq (0, 0, 0)$

| $\omega(r)$ | $t_0$ | $q$ |
|---|---|---|
| 96 | 5 | 171659 |
| 25 | 3 | 7447 |
| 20 | 3 | 4566 |
| 19 | 3 | 4100 |

For $q = 2, 4, 8, 16, 32, 64, 3, 9, 27, 81$, and any given 3-tuple $(\sigma_1, \sigma_2, \sigma_3) \in F_q^3$, we find a primitive polynomial of degree 7 over $F_q$ with the first three coefficients prescribed as $\sigma_1, \sigma_2, \sigma_3$ by computer search. For $q = 2^8$, we find a primitive polynomial of degree 7 over $F_{2^8}$ with the first three coefficients prescribed as $(0, 0, 0)$. So we have

**Theorem 10.** *Let $p = 2, 3$, $q$ a power of $p$. There exists a primitive polynomial of degree 7 over $F_q$ with the first three coefficients prescribed.*

## References

[1] W.S. Chou, S.D. Cohen, Primitive elements with zero traces, Dedicated to Professor Ko Chao on the occasion of his 90th birthday, Finite Fields Appl. 7 (2001) 125–141.
[2] S.D. Cohen, Primitive elements and polynomials with arbitrary trace, Discrete Math. 83 (1990) 1–7.
[3] S.D. Cohen, in: G.L. Mullen, P.J. Shiue (Eds.), Primitive Elements and Polynomials: Existence results, Lecture Notes in Pure & Applied Math., Vol. 141, Marcel Dekker, New York, 1993, pp. 43–55.
[4] S.D. Cohen, D. Mills, Primitive polynomials with the first and second coefficients prescribed, preprint.
[5] Sh.Q. Fan, W.B. Han, Character sums over Galois rings and primitive polynomials over finite fields, Finite Fields Appl. S1071-5797(03)00041-8, in press.
[6] Sh.Q. Fan, W.B. Han, *p*-adic formal series and primitive polynomials over finite fields, Proc. Amer. Math. Soc. 132 (1) (2004) 15–31.
[7] Sh.Q. Fan, W.B. Han, *p*-adic formal series and Cohen's problem, Glasgow Math. J. in press.
[8] Sh.Q. Fan, W.B. Han, Primitive polynomials over finite fields of characteristic two, Appl. Algebra Eng. Commun. Comput., in press.
[9] W.B. Han, The coefficients of primitive polynomials over finite fields, Math. Comp. 65 (213) (1996) 331–340.
[10] W.B. Han, On Cohen's problem, Advance in Cryptology—Chinacrypt'96, Chinese Academic Press, 1996, (in Chinese) 231–235.

[11] W.B. Han, On two exponential sums and their applications, Finite Fields Appl. 3 (1997) 115–130.
[12] T. Hansen, G.L. Mullen, Primitive polynomials over finite fields, Math. Comp. 59 (200) (1992) 639–643 Supplement: S47-S50.
[13] D. Jungnickel, S.A. Vanstone, On primitive polynomials over finite fields, J. Algebra 124 (1989) 337–353.
[14] P.V. Kumar, T. Helleseth, A.R. Calderbank, An upper bound for Weil exponential sums over Galois rings and applications, IEEE Trans. Inform. Theory 41 (2) (1995) 456–468.
[15] W.-C.W. Li, Character sums over *p*-adic fields, J. Number Theory 74 (1999) 181–229.
[16] D. Mills, Existence of primitive polynomials with three coefficients prescribed, J. Algebra Number Theory Appl., in press.